CLAIMS

We Claim:

1. A secure digital appliance comprising:

a network interface for receiving communications coupled over a communication network;

provision for private key storage, said provision for private key storage operable to securely store a private key of a private key and public key pair;

a decryption module coupled to said network interface and coupled to said provision for private key storage, said decryption module operable upon receiving a message that is encrypted using said public key to decrypt said message using said private key for obtaining a first secret key, said decryption module also operable to decrypt encrypted digital content that is received at said network interface using said first secret key so as to obtain digital content;

a local output device coupled to said decryption module, said local output device operable to provide protected output of said digital content, said secure digital appliance not allowing for any output of said digital content other than said protected output.

2. The secure digital appliance of Claim 1 further comprising:

a decode module coupled to said decryption module and operable to decode said digital content when said digital content is encoded; and

a local output interface coupled to said decode module and coupled to said local output device for output of said decoded digital content.

3. The secure digital appliance of Claim 1 further including:

an integrated circuit device, said provision for private key storage, said decryption module and said decode module included in said integrated circuit device.

4. The secure digital appliance of Claim 1 wherein said protected output provides for exhibition of said digital content.

5. The secure digital appliance of Claim 4 wherein said secure digital appliance does not contain any provision for output other than said exhibition of said digital content.

6. The secure digital appliance of Claim 5 wherein, upon receiving additional digital messages that are encrypted with said first secret key and that include additional secret keys, said decryption module is operable to decrypt said additional digital messages to obtain said additional secret keys, and further wherein, upon receiving digital content that is encrypted using said additional secret keys, said decryption module is operable to decrypt said encrypted digital content using ones of said additional secret keys so as to obtain said digital content.

7. The secure digital appliance of Claim 1 wherein, upon receiving a message that includes one or more time stamp, said secure digital appliance is

operable to only exhibit said digital content during the time indicated by said one or more time stamp.

8. A method for protecting digital content comprising:

upon receiving a request for digital content that identifies a secure digital appliance that contains a private key of a private key and public key pair, determining said public key;

sending a first digital message to said secure digital appliance, said first digital message encrypted with said public key and said first digital message including a first secret key;

decrypting said first digital message at said secure digital appliance using said private key so as to obtain said first secret key;

decrypting encrypted digital content at said secure digital appliance using said first secret key so as to obtain said digital content; and

providing for protected output of said digital content at said secure digital appliance, said secure digital appliance not allowing for any output of said digital content other than said protected output.

9. A method for protecting digital content as recited in Claim 8 further comprising:

decoding said encrypted digital content when said digital content requires decoding.

10. A method for protecting digital content as recited in Claim 9 further comprising:

verifying that said secure digital appliance will provide adequate protection of said digital content; and

not sending said first digital message and said digital content when said secure digital appliance is determined not to provide adequate protection of said digital content.

11. A method for protecting digital content as recited in Claim 8 wherein said protected output provides for exhibition of said digital content and wherein said secure digital appliance does not contain any provision for output other than said exhibition of said digital content.

12. A method for protecting digital content as recited in Claim 10 further comprising:

sending a second digital message to said secure digital appliance, said second digital message encrypted with said first secret key and said second digital message including a second secret key;

decrypting said second digital message at said secure digital appliance using said first secret key so as to obtain said second secret key; and

wherein said step of decrypting encrypted digital content at said secure digital appliance is performed using said second secret key.

13. A method for protecting digital content as recited in Claim 12 further comprising:

sending a third digital message to said secure digital appliance, said third digital message encrypted with said second secret key and said third digital message including a third secret key;

decrypting said third digital message at said secure digital appliance using said second secret key so as to obtain said third secret key; and

wherein said step of decrypting encrypted digital content at said secure digital appliance is performed using said third secret key.

14. A method for protecting digital content as recited in Claim 12 further comprising:

sending a plurality of additional digital messages to said secure digital appliance that include additional secret keys, each of said additional digital messages encrypted with said first secret key;

decrypting said plurality of additional messages at said secure digital appliance using said first secret key; and

wherein said step of decrypting encrypted digital content further comprises decrypting digital content that is encrypted using said additional secret keys at said secure digital appliance using ones of said additional secret keys so as to obtain said digital content.

15. A method for protecting digital content as recited in Claim 14 wherein said additional secret keys are used in a sequential manner to sequentially decrypt said encrypted digital content.

16. A method for protecting digital content as recited in Claim 10 further comprising the step of:

when said first digital message includes one or more time stamp, only allowing the exhibition of said digital content during the time indicated by said one or more time stamp.

17. A method for assuring protection of digital content comprising the steps of:

upon receiving a request for digital content that identifies a secure digital appliance that contains a private key of a private key and public key pair, and that identifies a set-top box that contains a private key of a private key and public key pair, determining said public key for said secure digital appliance and determining said public key for said set-top box;

sending a first digital message that is encrypted with said public key for said set-top box to said set-top box, said first digital message including a first secret key,

sending a second digital message that is encrypted with said public key for said secure digital appliance to said secure digital appliance, said second digital message including said first secret key,

decrypting said first digital message at said set-top box using said private key for said set-top box so as to obtain said first secret key;

decrypting digital content that is encrypted using said first secret key at said set-top box so as to obtain decrypted digital content;

decoding said decrypted digital content at said set-top box so as to obtain decoded digital content;

encrypting said decoded digital content at said set-top box using said secret key and sending said encrypted decoded digital content to said secure digital appliance;

decrypting said first digital message at said secure digital appliance using said private key for said secure digital appliance so as to obtain said first secret key;

decrypting said encrypted decoded digital content at said secure digital appliance using said first secret key so as to obtain said digital content; and

providing for protected output of said digital content at said secure digital appliance, said secure digital appliance not allowing for any output of said digital content other than said protected output.

18. The method of Claim 17 wherein said protected output further comprises exhibiting said digital content, said secure digital appliance not allowing for any output of said digital content other than said protected output.

19. A method for protecting digital content as recited in Claim 18 further comprising the step of:

verifying that said secure digital appliance and said set-top box will provide adequate protection of said digital content; and

not sending said digital content when either said secure digital appliance or said set-top box are determined not to provide adequate protection of said digital content.

20. The method of Claim 18 further comprising:

sending a plurality of additional digital messages to said set-top box, said plurality of additional digital messages encrypted with said first secret key and including additional secret keys; and

wherein said step of decrypting digital content further comprises decrypting digital content that is encrypted using said additional secret keys at said secure digital appliance using ones of said additional secret keys so as to obtain said digital content.